SOLUZIONE – ESERCIZIO WEEK17 CONSEGNA 1

Al fine di sfruttare la vulnerabilità, dobbiamo trovare un exploit di Metasploit che faccia al caso nostro.

Per farlo utilizziamo la keyword «search» unitamente al codice della vulnerabilità MS08_067.

Questo ci permette di controllare nel DB di Metasploit per eventuali exploit pubblici. Identifichiamo un unico exploit.

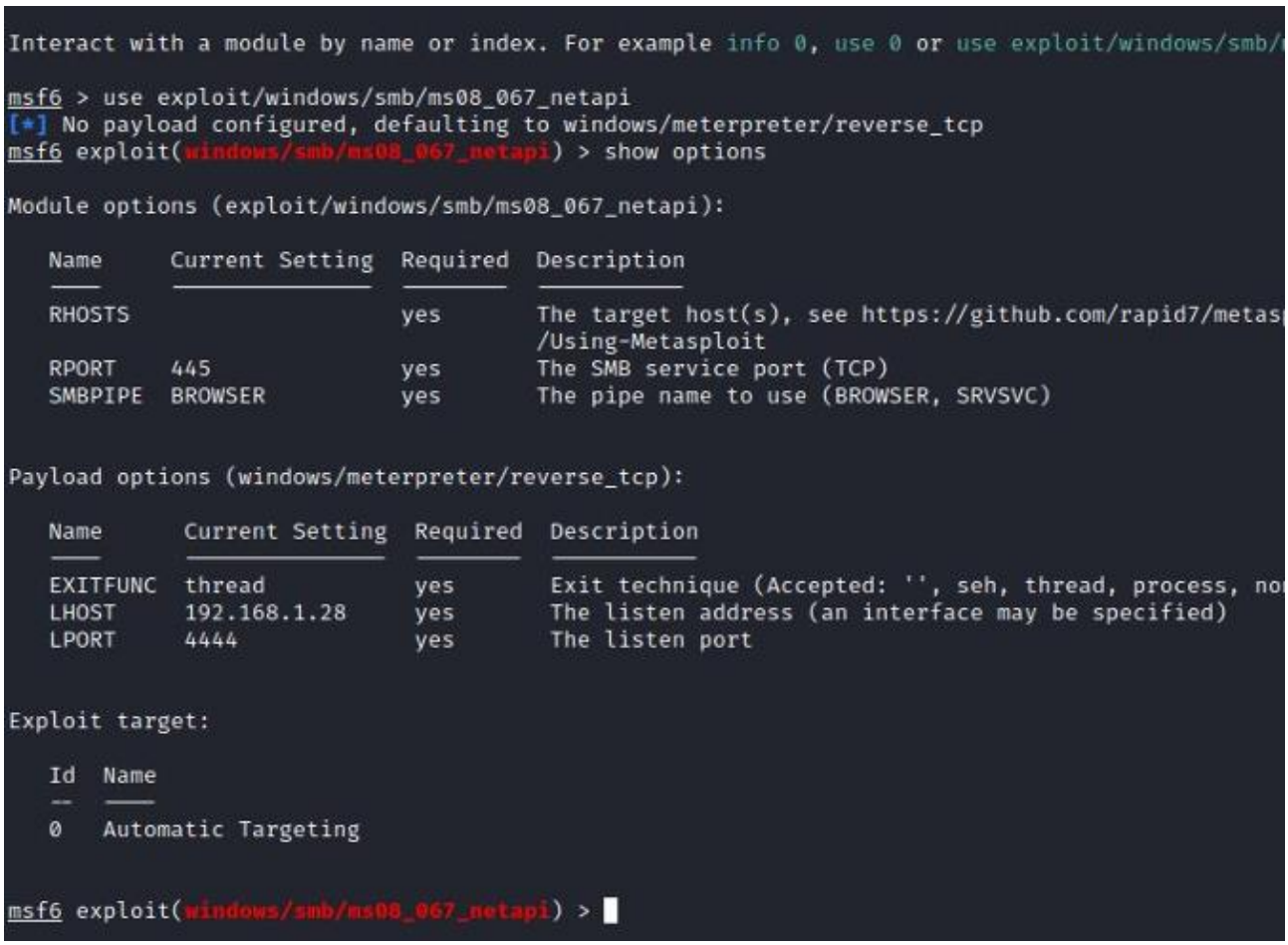
Possiamo utilizzarlo con il comando «use» seguito dal path dell'exploit, successivamente controlleremo i parametri necessari per eseguirlo.

Come spesso accade, l'exploit ha bisogno dell'IP della macchina Target per essere eseguito, dunque configuriamo il parametro «RHOSTS» in base alla nostra configurazione di rete.

Contestualmente vediamo che è stato scelto di default il payload Meterpreter/reverse_tcp come, per il quale bisogna configurare il parametro «LHOST».I parametri si configurano con la keyword «set» seguiti dal nome del parametro e dal valore che vogliamo assegnare al parametro.

Ad esempio, se il remote host (RHOSTS) ha l'IP 192.168.1.200,

scriveremo «set RHOSTS 192.168.1.200»



Una volta configurato il parametro «LHOST» per il payload con l'indirizzo della Kali Linux, eseguiamo l'attacco con il comando «exploit» per ottenere una sessione di Meterpreter.

Possiamo recuperare lo screenshot sulla macchina remota utilizzando il comando «screenshot» dalla sessione Meterpreter

Mentre possiamo verificare la presenza di webcam sulla macchina target eseguendo il comando «webcam_list»